EXHIBIT A

SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NEW YORK

MICHAEL BERNSTEIN, on behalf of himself and all others similarly situated,

Plaintiff,

v.

THE GLOBAL ATLANTIC FINANCIAL GROUP. LLC,

Defendant.

Index No. 159108/2023

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Michael Bernstein ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against The Global Atlantic Financial Group LLC ("Global Atlantic" or "Defendant"), and alleges, upon personal knowledge as to his own actions and the investigation of counsel, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises from a recent cyberattack and data breach (the "Data Breach") resulting in the acquisition of sensitive and private information in the possession and custody and/or control of Global Atlantic.

2. Plaintiff received a letter dated July 28, 2023 (the "Notice Letter") from Global Atlantic informing him that sensitive private information he had supplied to Global Atlantic, including his name, social security number, date of birth, and policy number(s) (collectively "personal identifying information" or "PII"), were illegally accessed and downloaded by cybercriminals who breached a MOVEit transfer server belonging to Pension Benefits Information

LLC ("PBI"), a third-party vendor that provides services to insurance companies such as Global Atlantic's subsidiaries. The Notice Letter is attached hereto as **Exhibit A**.

3. According to the Notice Letter, the Data Breach occurred on May 29 and May 30, 2023, and was discovered by PBI following disclosure from Progress Software, the creator of the MOVEit file transfer application, that criminals had exploited an "unknown vulnerability" in the application. PBI notified Global Atlantic on June 7, 2023 "that personal data for an uncertain number of policyholders had likely been taken by the cyber criminals."

4. The Data Breach exposed Defendant's negligence and breach of legal and equitable duties to protect and safeguard the sensitive PII from unauthorized access and exfiltration. Defendant failed to protect, encrypt or even redact this private information, leaving Plaintiff and other customers of Defendant exposed to drastically heightened risk of identity theft. The present and continuing risk to victims of the Data Breach will last throughout their respective lifetimes.

5. Defendant's Notice Letter downplayed the nature of the breach and the threat that it posed to victims whose Private Information was illicitly accessed and stolen. Defendant failed to tell its consumers how many people were impacted, how the breach occurred, or why Defendant took nearly two (2) months to begin notifying victims that hackers had gained access to their Private Information.

6. Defendant's failure to timely report the Data Breach made its customers more vulnerable to identity theft, as those customers received no warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their stolen PII.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance to mitigate the effects of the infiltrators misusing their PII.

8. By failing to adequately protect Plaintiff's and the Class's Private Information, failing to adequately notify them about the breach, and by obscuring the nature of the breach, Defendant violated state and federal law and harmed an unknown number of their customers.

9. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cybersecurity measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their Private Information, but Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent or mitigate the impact of the Data Breach.

10. Following the Data Breach, the victims' Private Information is permanently exposed and unsecured.

11. Accordingly, Plaintiff, on his own behalf and on behalf of a class and subclass of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

JURISDICTION AND VENUE

12. This Court has jurisdiction over Defendant pursuant to Civil Practice Law and Rules ("CPLR") § 301 because Defendant maintains its principal places of business in the state of New York and/or conduct substantial business in the state of New York.

13. Venue is proper in this Court pursuant to CPLR § 503(c) because Defendant maintains its principal office within the County of New York.

PARTIES

14. Plaintiff Michael Bernstein is a citizen of New Jersey and is a victim of the Data Breach. He received a Notice Letter dated July 28, 2023.

15. Defendant, The Global Atlantic Financial Group, LLC, is a Bermuda limited liability company with its principal place of business located in New York, New York.

STATEMENT OF FACTS

Defendant's Business

16. Defendant markets itself as a "leading U.S. retirement and life insurance company[.]"

17. Plaintiff and Class Members are current and former Global Atlantic customers. Global Atlantic required that Plaintiff and Class Members provide their PII as a condition of receiving Global Atlantic's services.

18. The information held by Defendant in its computer systems or those of its vendors at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

19. Upon information and belief, Defendant made promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them as a condition of obtaining products and/or services at Defendant would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

20. Indeed, Defendant promises in their Privacy Policy that: "[p]rotecting your personal information and respecting your privacy is important to us. We respect your privacy rights and choices[.]" The Privacy Statement further states that "[t]o protect your information from unauthorized access and use, we have adopted security measures that comply with applicable law, and are reasonably designed to protect the availability, confidentiality, and integrity of your personal information."

21. Plaintiff and Class Members provided their PII to Defendant with the reasonable

expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

22. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

23. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its IT vendors and affiliates. Defendant has a legal duty to keep consumer's PII safe and confidential.

24. Defendant had obligations created by FTC Act, Gramm-Leach-Bliley Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

25. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach

27. In the Notice Letter, Defendant stated that:

> At Global Atlantic, we do our best to protect your personal information and ensure our business partners do the same. Despite these efforts, we have been informed by

> Pension Benefits Information LLC ("PBI") that they recently experienced a cybersecurity incident involving the MOVEit file transfer application, and that the incident has impacted our policyholder data. PBI is a third-party vendor that Global Atlantic uses to satisfy applicable regulatory obligations to identify the deaths of insured persons, which can impact premium payment obligations and benefit eligibility. PBI is one of hundreds of companies across a variety of industries that have been impacted by the MOVEit incident.
>
> **Based on our analysis of the impacted data, we believe that the following types of personal identifiable information related to you were impacted: Name, Social Security Number, Date of Birth, Policy Number(s).**

See Exhibit A attached hereto.

28. According to the Notice Letter, Defendant was notified of the Data Breach on June 7, 2023. However, Defendant did not send out notices to Plaintiff and Class Members until on or about July 28, 2023, almost two (2) months later.

29. Despite their duties and alleged commitments to safeguard Private Information as "leaders" within their industry, Defendant did not in fact follow industry standard practices or applicable law in securing consumers' Private Information, as evidenced by the Data Breach.

30. Defendant recognized the actual imminent harm and injury that flowed from the Data Breach, as acknowledged in the Notice Letter. However, Defendant offered merely two (2) years of complimentary credit monitoring and identity monitoring services to victims, which does not adequately begin to address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Private Information that cannot be changed, such as Social Security numbers.

31. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent

account activity on Plaintiff's and the Class's financial accounts.

32. Even with two years' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Private Information is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

33. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the insurance industry and in similar industries preceding the date of the breach.

34. In light of recent high profile data breaches at other insurance providers and similar companies that handle sensitive private information, Defendant knew or should have known that its electronic records and consumers' Private Information would be targeted by cybercriminals.

35. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

36. Indeed, cyberattacks against industries such as insurance and healthcare have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."

37. Cyberattacks on insurance providers and similar companies have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they

are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."

38. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

39. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

40. As a result of Defendant's failure to protect Plaintiff and the proposed Class Members' PII, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in their possession.

41. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

42. The value of Plaintiff's and the Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen Private Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

43. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

44. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

45. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

46. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify such information as Plaintiff's and the proposed Class's social security numbers, phone numbers, email addresses, and other unregulated

sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, which in this instance also includes social security numbers, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

47. Defendant disclosed the Private Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

48. Defendant's failure to promptly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

49. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

50. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of Private Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

51. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

52. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

54. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information constitutes an unfair act or practice

prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Comply with Industry Standards

55. As noted above, experts studying cybersecurity routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

56. Several best practices have been identified that at a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

57. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

58. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards

in reasonable cybersecurity readiness.

59. The foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

60. Plaintiffs bring this action as a class action pursuant to Article 9 of the CPLR on behalf of a Nationwide Class and a New Jersey Subclass defined as:

> The Nationwide Class is defined as: All individuals who received a Notice Letter from Defendant notifying them that their PII was compromised in the Data Breach.
>
> The New Jersey Subclass is defined as:
>
> All individuals residing in New Jersey who received a Notice Letter, notifying them that their PII was compromised in the Data Breach

61. Excluded from the Class and Subclass are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

62. Plaintiff reserves the right to amend the class and subclass definitions.

63. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under CPLR Article 9.

a. **Numerosity**. The members of the Class and Subclass are so numerous that joinder would be impracticable. The exact number of class members is unknown to Plaintiff, but may exceed two million, based upon Defendant's total number of customers;

b. **Ascertainability**. Members of the Class and Subclass are readily identifiable

from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class and subclass claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's and Subclass's interests. His interests do not conflict with the Class's and Subclass's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's and Subclass's claims raise predominantly common fact and legal questions that a class-wide proceeding can answer for the Class and Subclass. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing Private Information;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's Private Information;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class and Subclass are entitled to damages, treble damages, or injunctive relief.

64. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence

65. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

66. Plaintiff and members of the Class entrusted their Private Information to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the Private Information in their care and custody, including following FTC guidelines and implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access. This includes following the FTC guidance on deleting Private Information that is no longer needed.

67. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their Private Information in

accordance with state-of-the-art industry standards concerning data security would result in the compromise of that Private Information —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's Private Information by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

68. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their Private Information. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

69. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's Private Information.

70. The risk that unauthorized persons would attempt to gain access to Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, much of it over long periods of time without any valid business or medical purpose, it was inevitable that unauthorized individuals would attempt to access Defendant's databases

containing the Private Information, whether by malware or otherwise.

71. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiff and the Class and the importance of exercising reasonable care in handling it and timely deleting any Private Information that was no longer needed.

72. Defendant breached its duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

73. Defendant's breach of its common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*

74. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

75. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Private Information.

76. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers' Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Private Information.

77. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

78. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its consumers, which is recognized by laws and regulations as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach, but failed to do so.

79. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

80. Defendant violated its duty under Section 5 of the FTC Act by failing to use

reasonable measures to protect Plaintiff's and the Class's Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

81. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

82. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

83. The injury and harm suffered by Plaintiff and members of the Class and Subclass were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to fulfill its duties and that such a breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

84. Had Plaintiff and the Class known that Defendant did not adequately protect their Private Information, Plaintiff and members of the Class would not have entrusted Defendant with their Private Information.

85. Defendant's various violations and their failure to comply with applicable laws and regulations constitute negligence *per se*.

86. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the

Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Private Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Private Information, entitling them to damages in an amount to be proven at trial.

87. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect their Private Information in their continued possession.

COUNT III
Breach of Contract

88. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

89. Defendant entered into contracts with Plaintiff and Class Members. Defendant breached these contracts when they failed to use reasonable data security measures that could have protected Plaintiff's and Class Members' private information from exposure and compromise in the Data Breach.

90. As a reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant's failure to use reasonable data security measures to store their Private Information, including but not limited to, the actual harm through the loss of their Private Information to cybercriminals.

91. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV
Unjust Enrichment

92. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

93. Plaintiff and members of the Class conferred a benefit upon Defendant in providing Private Information to Defendant.

94. Defendant appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's Private Information, as this was used to facilitate the services and goods it sold to its consumers, including Plaintiff's and the Class.

95. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the Class's Private Information because Defendant failed to adequately protect their Private Information. Plaintiff and the proposed Class would not have provided their Private Information to Defendant had they known Defendant would not adequately protect their Private Information.

96. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Violation Of The New York Deceptive Trade Practices Act ("GBL")
(New York Gen. Bus. Law § 349)

97. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

98. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law §

349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiff and the Class by representing that it would maintain adequate data privacy and security practices and procedures to safeguard Class Members' Private Information from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the Class by representing that it did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' Private Information;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' Private Information;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' Private Information, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa (2).

99. Defendant knew or should have known that its data security practices were inadequate to safeguard Class Members' Private Information entrusted to it, and that the risk of a data breach or theft was highly likely.

100. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

101. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) regarding Defendant's aggregation and handling of Private Information, including but not limited to failing to encrypt, redact, and/or otherwise protect that information.

102. The representations upon which consumers (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of Private Information), and consumers (including Plaintiff and Class Members) relied on those representations to their detriment.

103. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

104. Defendant knew or should have known that its data security practices were inadequate to safeguard Class Members' Private Information and that the risk of a data security incident was high.

105. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing insurance services to consumers in the State of New York.

106. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and continuing to cause damages to Plaintiff and the Class.

107. As a direct and proximate result of Defendant's multiple, separate violations of

GBL §349, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including the cost of credit and identity theft monitoring as well as loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Private Information; and (h) the continued and substantial risk to Plaintiff's and Class Members' Private Information, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' Private Information.

108. As a result, Plaintiff and Class Members have been damaged in an amount to be proven at trial.

109. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

110. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h),

including, but not limited to, actual damages, treble damages, statutory damages, in junctive relief, and/or attorney's fees and costs.

111. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

112. As a direct result of Defendant's violation of GBL § 349, Plaintiff and Class Members are also entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT VI
Violation Of New York Gen. Bus. Law § 899-aa

113. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

114. According to the Notice Letter, Defendant learned of the Data Breach on June 7, 2023, but did not notify Plaintiff and Class Members until on or about July 28, 2023.

115. Pursuant to Gen. Bus. Law § 899-aa(2), Defendant was required to provide disclosure to the victims of a data breach within "the most expedient time possible and without unreasonable delay. . . ."

116. Defendant violated the statute by waiting almost two (2) months to notify Plaintiff and Class Members of the data breach.

117. As a result of Defendant's unwarranted and unreasonable delay in notifying the data breach victims, the victims were unaware that their Private Information had been illegally accessed and stolen and that they were at drastically increased risk of being subject to identity

theft. Had they known sooner, they could have taken immediate steps to protect their identities and prevent further injury.

118. As a result of the Defendant's violation of the statute, Plaintiff and Class Members were injured and demand all remedies warranted by law.

COUNT VII
Violation Of The New Jersey Consumer Fraud Act
(N.J. Stat. Ann. § 56:8-1 *et seq.*)
(On Behalf of the New Jersey Subclass)

119. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

120. The deceptive and misleading statements set forth above are advertisements within the meaning of N.J. Stat. Ann. § 56:8-1(a).

121. Defendant is a "person" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

122. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, et seq., prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

123. Defendant's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New Jersey Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy

measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' Private Information, including duties imposed by the FTC and industry-standard procedures, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' Private Information, including duties imposed by the FTC and industry-standard procedures;

f. Failing to timely and adequately notify Plaintiff and New Jersey Subclass Members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and New Jersey Subclass Members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff's and New Jersey Subclass Members' Private Information, including duties imposed by the FTC and industry-standard procedures.

124. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

125. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and New Jersey Subclass Members, that their Private Information was not exposed and misled Plaintiffs and New Jersey Subclass Members into believing they did not need to take actions to secure their identities.

126. Defendant intended to mislead Plaintiff and New Jersey Subclass Members and induce them to rely on their misrepresentations and omissions.

127. Defendant acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's and New Jersey Subclass Members' rights.

128. As a direct and proximate result of Defendant's unconscionable and deceptive practices, Plaintiff and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; the expense of purchasing multi-year identify theft protection; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

129. Plaintiff and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

COUNT VIII
Violation of the New Jersey Customer Security Breach Disclosure Act,
(N.J. Stat. Ann. §§ 56:8-163 *et seq.*)
(On Behalf of the New Jersey Subclass)

130. Plaintiff incorporates by reference and realleges each and every allegation contained above, as though fully set forth herein.

131. Defendant is a business that compiles or maintains computerized records that include "personal information" on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

132. Plaintiff's and New Jersey Subclass Members' Private Information includes "personal information" covered under N.J. Stat. Ann. §§ 56:8-163, et seq.

133. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person."

134. Because Defendant discovered a breach of their security system in which Private Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Private Information was not secured, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, et seq.

135. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated N.J. Stat. Ann. § 56:8-163(b).

136. As a direct and proximate result of Defendant's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass Members suffered the damages described above.

137. Plaintiff and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class and Subclass, appointing Plaintiff as class and subclass representative, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

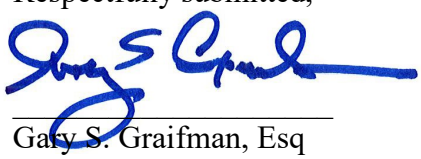
H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: September 15, 2023

Respectfully submitted,



Gary S. Graifman, Esq
Kantrowitz Goldhamer & Graifman, P.C.
16 Squadron Blvd., Suite 106
New City, NY 10956
Tel: (845) 356-2570, X129
Fax: (845 356-4335
Email: ggraifman@kgglaw.com

Howard T. Longman, Esq.
Longman Law, P.C.
354 Eisenhower Parkway, Suite 1800
Livingston, New Jersey 07039
Tel: (973) 994-2315
Fax: (973) 994-2319
Email: hlongman@longman.law

Attorneys for Plaintiff & the Proposed Class and Subclass

The Global Atlantic Financial Group LLC
Accordia Life and Annuity Company
Commonwealth Annuity and Life Insurance Company
First Allmerica Financial Life Insurance Company
Forethought Life Insurance Company
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 28, 2023

J7450-L01-0357408 T01194 P023 *******ALL FOR AADC 07099
MICHAEL BERNSTEIN
[redacted]

RE: NOTICE OF CYBERSECURITY INCIDENT

Dear Michael Bernstein:

At Global Atlantic, we do our best to protect your personal information and ensure our business partners do the same. Despite these efforts, we have been informed by Pension Benefits Information LLC ("PBI") that they recently experienced a cybersecurity incident involving the MOVEit file transfer application, and that the incident has impacted our policyholder data. PBI is a third-party vendor that Global Atlantic uses to satisfy applicable regulatory obligations to identify the deaths of insured persons, which can impact premium payment obligations and benefit eligibility. PBI is one of hundreds of companies across a variety of industries that have been impacted by the MOVEit incident.

Based on our analysis of the impacted data, we believe that the following types of personal identifiable information related to you were impacted: Name, Social Security Number, Date of Birth, Policy Number(s).

Please note that Global Atlantic's environment was *not* compromised as a part of this incident. It is still safe to interact with our corporate systems and our website.

While we have no indication of identity theft or fraud related to this event, we take your personal information and privacy seriously. To help you protect your identity, **we are offering you a two-year membership in Experian's® IdentityWorks℠**. This product provides you with superior identity theft detection and resolution of identity theft.

The following pages of this letter provide information about the incident, our response, and resources available to help you protect your information, including details about your two-year Experian® IdentityWorks℠ membership.

Recommended next steps

Review the enclosed information and activate your complimentary two-year membership to start monitoring your personal information with Experian's® IdentityWorks℠. To learn how, see the section below titled "Instructions on activating your membership with Experian's IdentityWorks℠."

We're here to help

If you have questions or need more information, please visit our FAQ page at www.globalatlantic.com/MOVEit or contact Experian's customer care team at 833-919-4754 toll-free Monday through Friday from 8:00 a.m. – 10:00 p.m. Central, or Saturday and Sunday from 10:00 a.m. – 7:00 p.m. Central. Be prepared to provide your engagement number B098720.

Sincerely,

Rob Arena
Co-President

Global Atlantic Financial Group (Global Atlantic) is the marketing name for The Global Atlantic Financial Group LLC and its subsidiaries, including Accordia Life and Annuity Company, Commonwealth Annuity and Life Insurance Company, First Allmerica Financial Life Insurance Company, and Forethought Life Insurance Company.

0357408

What happened? On or around May 31, 2023, Progress Software disclosed that cyber criminals had actively exploited an unknown vulnerability in its MOVEit file transfer application. Because MOVEit is used by thousands of organizations to support the secure transfer of data for common business activities, this incident has affected many companies around the world. One of the organizations impacted by the MOVEit incident is PBI. PBI is a third-party vendor that provides services to insurance companies, including subsidiaries of Global Atlantic.

Upon learning of the incident, PBI initiated an investigation, which revealed that cyber criminals accessed one of their MOVEit transfer servers on May 29 and May 30, 2023, and downloaded certain data from that system. On June 7, 2023, PBI notified Global Atlantic that personal data for an uncertain number of policyholders had likely been taken by the cyber criminals.

What information was involved? Based on our analysis of the impacted data, we believe that the following categories of personal identifiable information related to you were impacted: **Name, Social Security Number, Date of Birth, Policy Number(s).**

What we are doing. Upon learning of this incident, our organization engaged outside experts and has worked with PBI to understand the nature and scope of information impacted. We have also reported the incident to the appropriate authorities.

To help protect your identity, we are offering a complimentary two-year membership in Experian's® IdentityWorks℠.

What you can do. Review the instructions below and activate your complimentary two-year membership to start monitoring your personal information with Experian's® IdentityWorks℠. As always, you should remain vigilant and be on the alert for suspicious activity by reviewing your financial account statements and monitoring free credit reports to ensure there are no transactions or other activities that you did not initiate or authorize. You should report any suspicious activity to your financial advisor or the appropriate service provider.

Other important information. You can obtain information about data security, avoiding or preventing identity theft, or obtaining fraud alerts or a credit freeze from the Federal Trade Commission, your state Attorney General, and the three credit reporting agencies listed on the next page:

Federal Trade Commission	Attorney General
You can contact the Federal Trade Commission at: www.identitytheft.gov 600 Pennsylvania Avenue, NW Washington, DC 20580 1-877-ID-THEFT (1-877-438-4338) 1-866-653-4261 (TTY)	You can contact the New Jersey Attorney General's Office at: njoag.gov 25 Market St Trenton, NJ 08611 609-292-4925

You are advised to contact local law enforcement, your state Attorney General's Office, or the Federal Trade Commission to report suspected incidents of identity theft. If you have been the victim of identity theft, you have the right to file or obtain a police report with your local police.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting agencies listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report. A "credit freeze" on a credit report will prohibit a credit reporting agency from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report.

To request a credit freeze, individuals may need to provide some or all of the following information to the credit reporting agency:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting agencies listed below:

Equifax	Experian	TransUnion LLC
Phone: 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/ Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Phone: 1-888-397-3742 https://www.experian.com/help/ Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	Phone: 1-800-916-8800 https://www.transunion.com/credit-help TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

This notice has not been delayed by law enforcement.

For More Information. If you have further questions or concerns please call 833-919-4754 toll-free Monday through Friday from 8:00 am – 10:00 pm Central, or Saturday and Sunday from 10:00 am – 7:00 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B098720.

0357408

Instructions on activating your membership with Experian's® IdentityWorks℠

To help protect your identity, we are offering complimentary access to Experian® IdentityWorks℠ for twenty-four (24) months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for twenty-four (24) months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24)-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Ensure that you enroll by October 31, 2023** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-919-4764 by October 31, 2023. Be prepared to provide engagement number B098720 as proof of eligibility for the Identity Restoration services by Experian.